Ben jij al klaar voor het
Normenkader Informatiebeveiliging en Privacy
voor het Funderend Onderwijs?

YourSafetynet IBP FO

YOURSAFETYNET

IBP-tooling® voor het funderend onderwijs
(primair- en voortgezet onderwijs)

YourSafetynet IBP: solide informatiebeveiliging en privacy (IBP) binnen het funderend onderwijs (FO)

Digitaal weerbaar

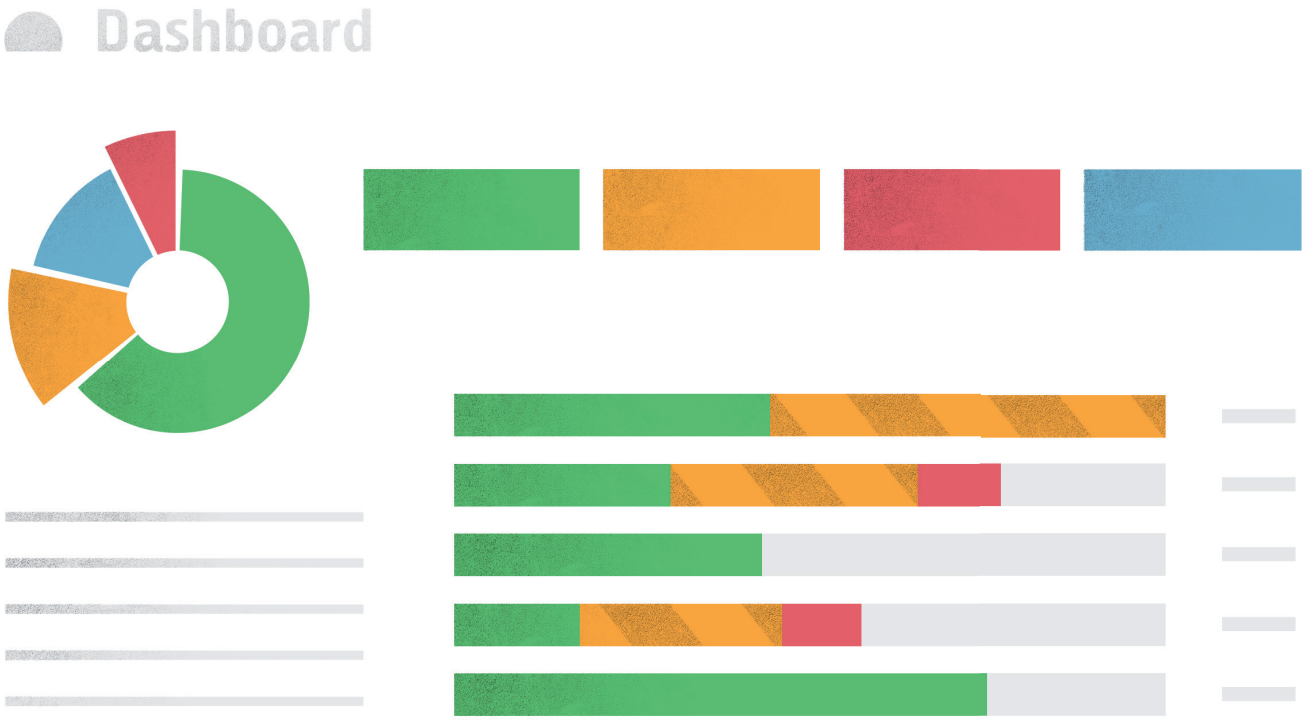
Van een digitaal leerling-administratiesysteem tot tablets en laptops in de klas: het funderend onderwijs ondergaat momenteel een razendsnelle digitalisering. Deze inzet van ICT biedt diverse educatieve en administratieve voordelen en mogelijkheden, maar brengt ook nieuwe kwetsbaarheden en risico's met zich mee. Het is daarom de verantwoordelijkheid van onderwijsinstellingen om deze risico's te beperken.

Algemene verordening gegevensbescherming

Volgens de Algemene verordening gegevensbescherming (AVG) moeten onderwijsinstellingen niet alleen zorgvuldig omgaan met privacygevoelige informatie ofwel persoonsgegevens, maar deze gegevens ook adequaat beveiligen. Leerlingen, ouders/verzorgers en medewerkers moeten erop kunnen vertrouwen dat hun persoonsgegevens veilig worden bewaard.

Om dit te bewerkstelligen moeten onderwijsinstellingen passende organisatorische en technische maatregelen nemen zoals de AVG vereist. Het onderwijs moet zijn digitale weerbaarheid vergroten en de cyberveiligheid verhogen. Daarom is het noodzakelijk dat alle instellingen aan een aantoonbaar veiligheidsniveau voldoen.

Het ministerie verplicht schoolbesturen om vanaf schooljaar 2023/2024 in hun jaarverslag expliciet aandacht te geven aan informatiebeveiliging en privacy. Dat zorgt ervoor dat besturen zich bewust worden van hun verantwoordelijkheid ten aanzien van digitale veiligheid en privacy.



Nieuw normenkader

Voor het verbeteren van de digitale veiligheid in het funderend onderwijs (overkoepelende term voor het primair- en voortgezet onderwijs), is een integrale en overkoepelende aanpak nodig. Dit houdt in dat onderwijsinstellingen zich moeten richten op het identificeren van risico's, het nemen van beschermende maatregelen, het detecteren van incidenten, het reageren op incidenten en het herstellen van eventuele schade. Het funderend onderwijs (FO) gaat, naar het voorbeeld van het MBO en HO, gebruik maken van een normenkader met een bijbehorend toetsingskader om te bepalen of aan de gestelde normen wordt voldaan. Maar scholen moeten wel weten hoe ze dat moeten aanpakken.

Het Normenkader Informatiebeveiliging en Privacy Funderend Onderwijs (IBP FO) is ontwikkeld door het ministerie van OCW, Kennisnet, SIVON, de PO-Raad en VO-raad vanuit het programma Digitaal Veilig Onderwijs. Dit normenkader beschrijft welke maatregelen onderwijsinstellingen moeten nemen om bepaalde risico's te verkleinen en het onderwijs digitaal veilig te maken. Het is onderverdeeld in een normenkader Informatiebeveiliging en een normenkader Privacy. Het normenkader Informatiebeveiliging is opgedeeld in maar liefst 15 domeinen en is daarmee ook een gids om grip te krijgen op cybersecurity.

Vrijblijvendheid is geen optie als het gaat om digitale weerbaarheid en privacy. Het is belangrijk dat alle betrokken partijen zich inzetten om de digitale weerbaarheid in de hele sector te verhogen en om de continuïteit en kwaliteit van het onderwijs en onderzoek te waarborgen. Onderwijsinstellingen moeten aan de slag gaan en het normenkader in de praktijk toepassen. Het verlagen van de beschreven risico's moet voldoen aan een baseline, wat betekent dat is bepaald welke maatregelen een onderwijsinstelling minimaal moet nemen of laten nemen.

IBP in de praktijk

Vrijblijvendheid is geen optie als het gaat om het vergroten van de digitale weerbaarheid en het goed regelen van privacy. Het is echter een uitdaging voor scholen om dit goed aan te pakken. Het implementeren van informatiebeveiliging en privacyregels in onderwijsinstellingen kan tijdrovend en kostbaar zijn vanwege complexe normen en wetgeving.

Grote uitdaging

Bovendien moeten onderwijsinstellingen genomen maatregelen aantoonbaar maken om te voldoen aan de Algemene verordening gegevensbescherming. Ook is dat noodzakelijk om zich te kunnen verantwoorden richting de Autoriteit Persoonsgegevens of de externe accountant. Het ontbreekt vaak aan inzicht in de voortgang en status van het IBP-traject. Dat maakt implementatie en borging lastig. Steeds meer signalen wijzen erop dat onderwijsinstellingen vaker het doelwit zijn van cyberaanvallen en beveiligingsincidenten, waardoor mogelijke datalekken enorme (herstel) kosten met zich mee kunnen brengen en de reputatie van de instelling kunnen schaden. Daarom is dit vanuit de praktijk een extra argument om het IBP-beleid goed op orde te hebben.

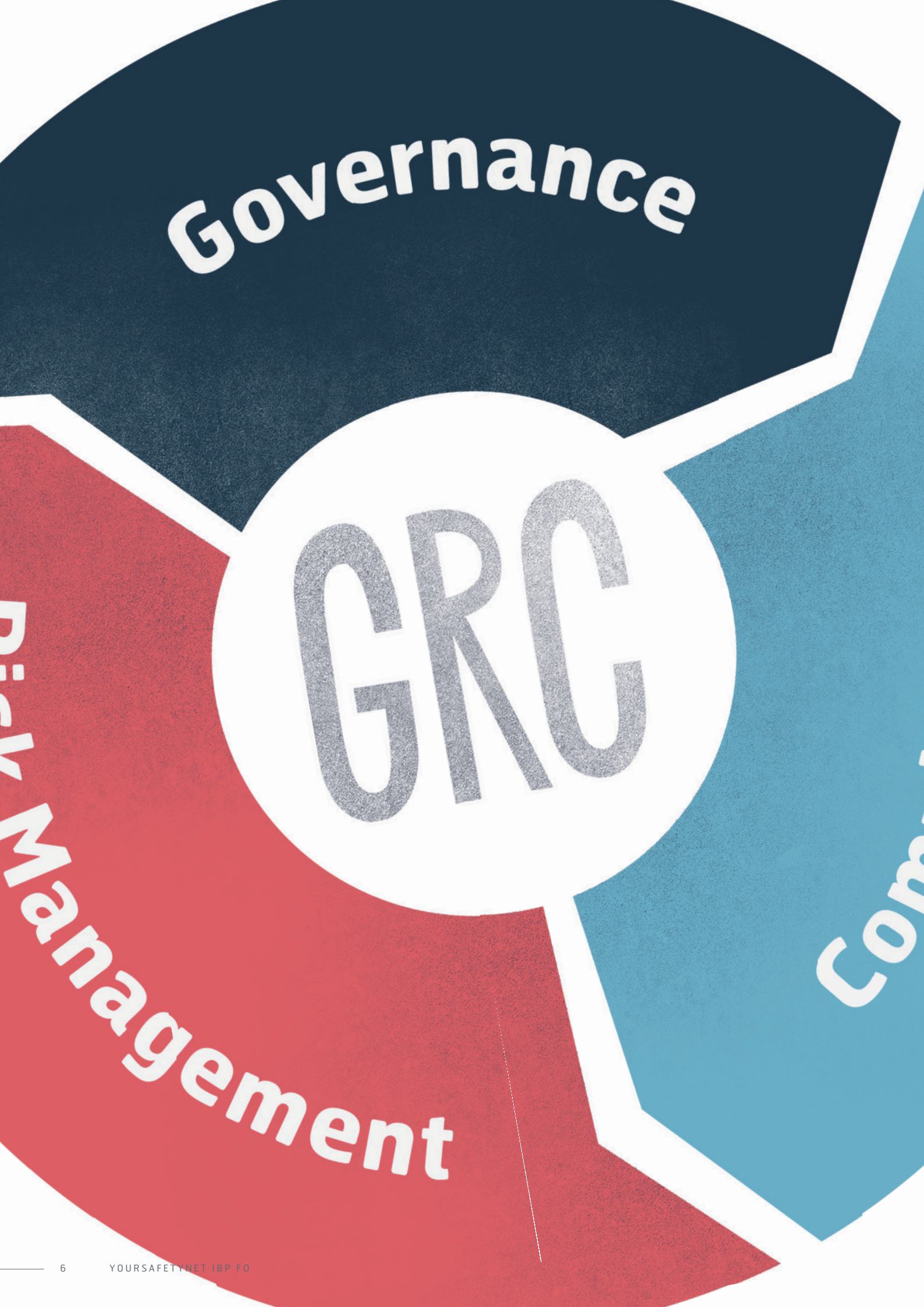
Verantwoordings- en informatieplicht onderwijsinstellingen

Instellingen moeten niet alleen verantwoording afleggen aan de Autoriteit Persoonsgegevens of externe accountants op basis van artikel 5.2 van de AVG, maar hebben ook een informatieplicht jegens leerlingen, ouders/verzorgers en medewerkers. Ze moeten volgens artikel 12-14 van de AVG transparant zijn over hoe zij de persoonsgegevens van betrokkenen verwerken.

Het implementeren en waarborgen van informatiebeveiliging en privacy binnen onderwijsinstellingen is een uitdaging. Vaak hebben de verantwoordelijken geen duidelijk inzicht in de voortgang en status van het IBP-traject. De IBP-tooling® biedt twee normenkaders (Informatiebeveiliging en Privacy) die onderwijsinstellingen helpen bij het krijgen van inzicht en overzicht in hun IBP-traject.

IBP tooling®

Voldoet jullie onderwijsinstelling al aan de Informatieplicht?


Governance
GRC
Risk Management

Governance, risk en compliance (GRC)

YourSafetynet IBP: eenvoudig ‘in control’

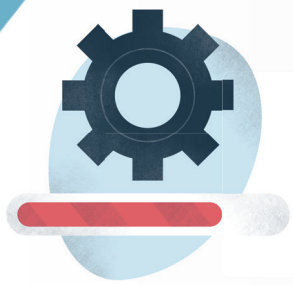
Samen met gespecialiseerde onderwijspartners die de knelpunten en aandachtspunten uit de praktijk goed kennen, hebben we een gebruiksvriendelijke tooling ontwikkeld voor Governance, Risk & Compliance (GRC-tool). YourSafetynet IBP is dé GRC-tool die besturen van onderwijsinstellingen binnen het primair en voortgezet onderwijs helpt bij het voldoen aan het Normenkader.

Met deze complete IBP-tooling® organiseer, structureer, presenteer en rapporteer je risico’s en maatregelen op het gebied van informatiebeveiliging en privacy. Ons uitgangspunt is gebruiksvriendelijkheid en functionaliteit. Deze mix heeft zich bewezen: al meer dan 250 onderwijsinstellingen maken inmiddels succesvol gebruik van deze tooling.

De oplossing begeleidt je stap voor stap zonder ingewikkelde handelingen door alle maatregelen die nodig zijn voor een goed geregelde informatiebeveiliging en privacy. De tooling focust zich daarbij op de pijlers beleid, processen en techniek. Door deze structuur wordt alles inzichtelijk en neemt YourSafetynet IBP veel werk uit handen. IBP is bovendien geen eenmalige oefening. Dankzij de geïntegreerde Plan Do Check Act-methode (PDCA) is IBP met minimale inspanningen te borgen binnen de onderwijsinstelling.

Stevig fundament

De tooling is ontwikkeld op een stevig fundament dat is gebaseerd op onderwijs- en privacywetgeving. We hebben verder gebouwd op dit fundament en de tooling uitgebreid. Het normenkader informatiebeveiliging voor het funderend onderwijs is hiervan het resultaat. Het privacy-normenkader voor het funderend onderwijs is nog niet beschikbaar. Zodra dit normenkader beschikbaar is, nemen we het in de tooling op. Tot die tijd ondersteunt de tooling de huidige aanpak IBP van Kennisnet. De templates uit het definitieve privacy-normenkader voor het FO zullen zoveel mogelijk aansluiten op de huidige aanpak IBP van Kennisnet. Of je nu al werkt met de huidige workflow op basis van de aanpak van Kennisnet of straks start met de workflow op basis van het normenkader privacy, in beide gevallen zijn gemaakte beleidsafspraken en procedures van toepassing. Deze werkzaamheden hoeven dus niet opnieuw te worden uitgevoerd.

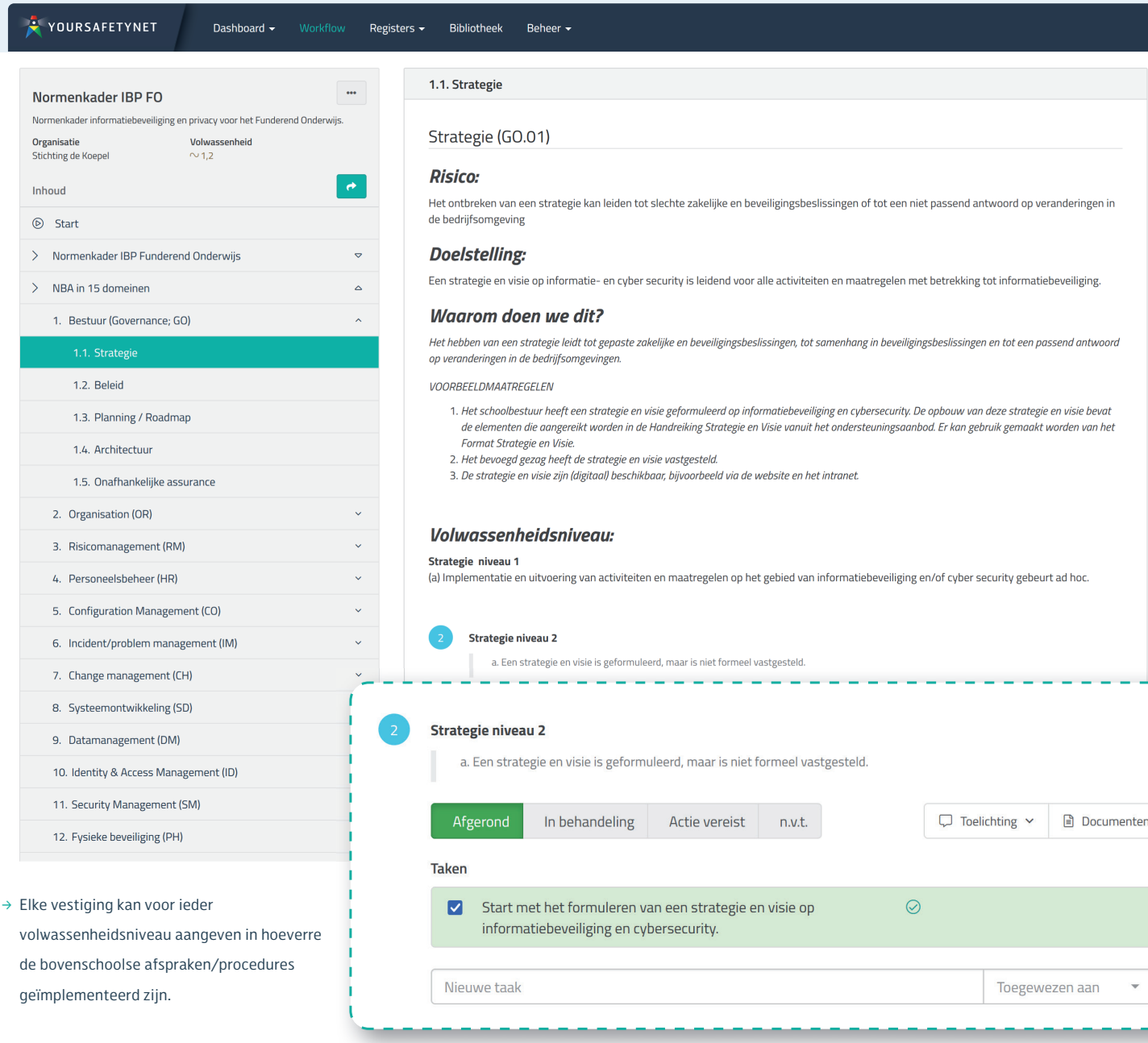


Update: Alle huidige gebruikers van YourSafetynet IBP Plus ontvangen de hier beschreven nieuwe versie van YourSafetynet IBP via een update.

De basis: IBP Workflow Wizard

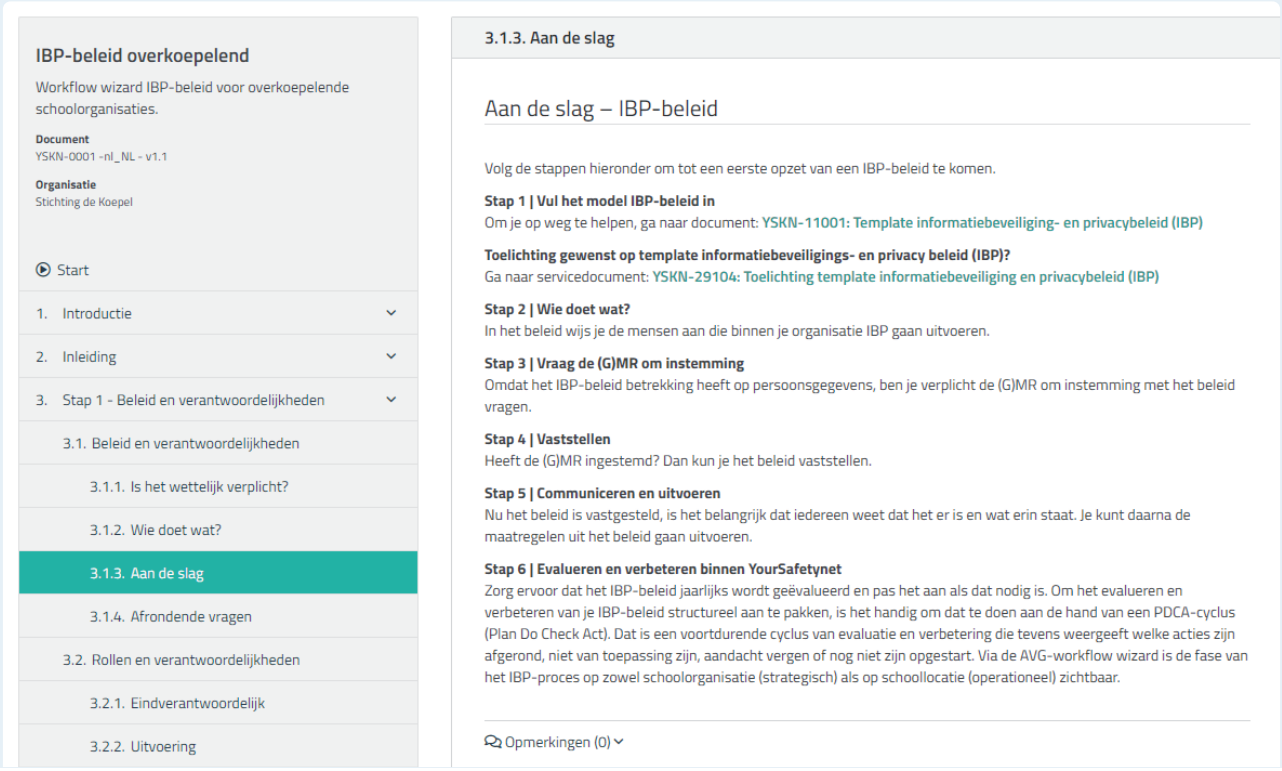
De kern van de oplossing is een overzichtelijke GRC-module: de IBP Workflow Wizard. Hiermee kan op bestuursniveau (het “masterniveau”) informatiebeveiliging en privacy goed worden geregeld. Elke workflow leidt je stap voor stap langs alle verplichte statements en vervolgens langs de maatregelen die op elk volwassenheidsniveau moeten worden genomen. De afspraken en procedures kunnen vervolgens eenvoudig naar de vestigingen/locaties worden uitgerold.

Voor elk statement en volwassenheidsniveau wordt op bovenschools niveau de status aangegeven, worden documenten gekoppeld en worden eventueel taken toegewezen met de gewenste doorlooptijd. Het uitgangspunt daarbij is om de afzonderlijke vestigingen/ locaties zo min mogelijk te belasten met onnodige of dubbele werkzaamheden en ingewikkelde materie. Elke vestiging kan via de workflow op schoollocatieniveau stap voor stap aangeven in hoeverre men de bovenschoolse afspraken/ procedures heeft geïmplementeerd.



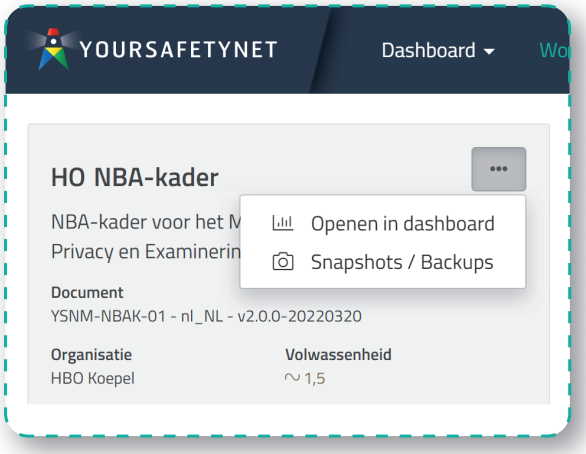
→ Elke vestiging kan voor ieder volwassenheidsniveau aangeven in hoeverre de bovenschoolse afspraken/procedures geïmplementeerd zijn.

→ De IBP Workflow Wizard leidt je stap voor stap langs alle IBP-maatregelen.



Blijf in control dankzij snapshots

Door middel van een snapshot kun je de status op een willekeurig moment “bevriezen” en een kopie maken van de status van je IBP-maatregelen en bewijsvoering op dat moment. Met deze technologie kun je wijzigingen en de status van de noodzakelijke IBP-maatregelen op twee of meer momenten vergelijken. Zo krijg je op detailniveau inzicht in de gerealiseerde verschillen tussen beide perioden. Zo krijgt de privacy officer of functionaris gegevensbescherming (FG) bijvoorbeeld een gedetailleerd beeld van de voortgang sinds het vorige meetmoment. Op basis daarvan is een jaarlijkse evaluatie of rapportage mogelijk.



De belangrijkste voordelen op een rij:

- Stapsgewijze regeling van IBP en naleving van privacywetgeving.
- Bespaar kosten, tijd en mankracht dankzij de logische IBP-processtructuur.
- Snel instappen dankzij integratie van ‘Aanpak IBP van Kennisnet’.
- Voorziet in het normenkader voor informatiebeveiliging voor het FO en voorbereid op het privacy-normenkader.
- Overzichtelijk dashboard dat waardevolle stuurinformatie biedt.
- Verklein security- en privacyrisico’s verder dankzij ISMS-tools.
- Stevige verankering in de organisatie dankzij de Plan Do Check Act-methode.
- Altijd voldoen aan de laatste wetgeving en best practices dankzij updates.
- Eenvoudige en gebruiksvriendelijke opzet.

→ Snapshots maken een vergelijking van de status van IBP-maatregelen tussen verschillende momenten mogelijk.

Aanvullende tools uit het ISMS voor nog meer privacy, veiligheid en gemak

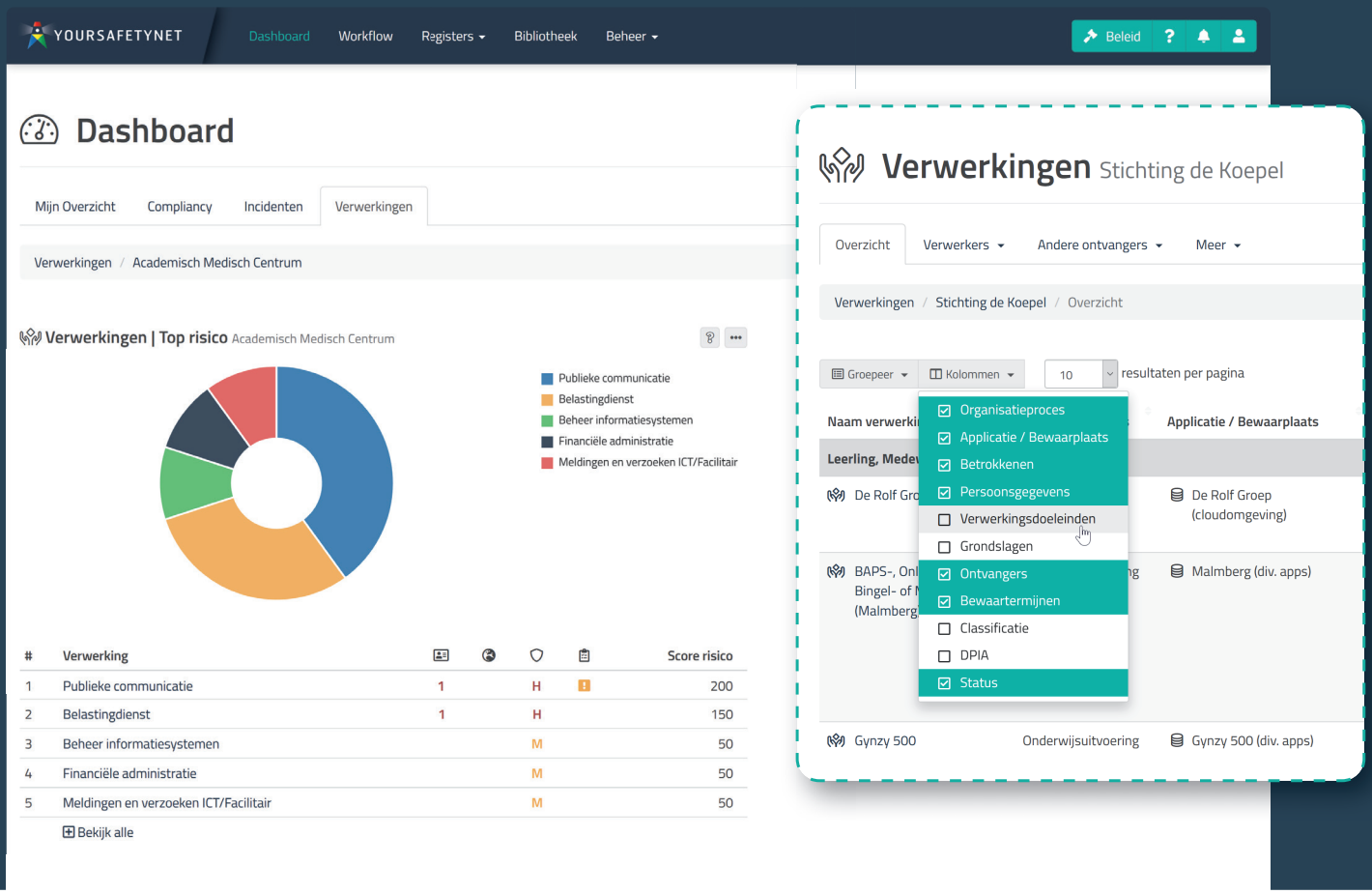
Naast de kernmodules biedt YourSafetynet ook aanvullende procestools voor IBP. Hiermee leveren we een belangrijke meerwaarde voor het gebruik van YourSafetynet, omdat deze modules de veiligheids- en privacyrisico's bij het verwerken van persoonsgegevens verder verkleinen en het IBP-traject nog eenvoudiger maken. Deze specifieke IBP-tools zijn procesonderdelen van het Information Security Management System (ISMS) en helpen onderwijsinstellingen bij het creëren, beheren en onderhouden van beleidsdocumenten, processen, procedures en werkinstructies om sneller, veiliger en gemakkelijker te voldoen aan de gestelde baseline.

YourSafetynet DPIA* Data Protection Impact Assessment

Wanneer je persoonsgegevens verwerkt, ben je verplicht om deze te beschermen met de juiste maatregelen. Dat moet gebeuren volgens de Algemene verordening gegevensbescherming. Wanneer de verwerking naar verwachting een hoog risico voor de betrokken oplevert, moet je het effect van het verwerken van persoonsgegevens op de privacy van de betrokkenen, zoals leerlingen, studenten en medewerkers, vooraf onderzoeken.

Dit onderzoek heet een Data Protection Impact Assessment (DPIA), of in het Nederlands een gegevensbeschermingseffectbeoordeling. Met een DPIA onderzoek je het effect van de verwerking van persoonsgegevens op de privacy van de betrokkenen en minimaliseer je zo de risico's op privacy-schending. We hebben YourSafetynet DPIA ontwikkeld om je daarbij te helpen. Deze tool is grotendeels gebaseerd op de handreiking en modellen voor het uitvoeren van een DPIA van SIVON en Kennisnet. De online workflow wizard begeleidt je stap voor stap door het evaluatieproces.

* Introductie in de loop van 2023



YourSafetynet RVV

Register van verwerkingsactiviteiten

Een voorbeeld van een aanvullende tool is YourSafetynet RVV. Dit register is voor onderwijsinstellingen verplicht vanuit de AVG, maar het opstellen en bijhouden van zo'n RVV is zonder speciale tooling een flinke klus. Daarom hebben we als onderdeel van het ISMS de module YourSafetynet RVV ontwikkeld. Deze online tool biedt een vooropgezet register waarin je veel verwerkers met slechts een paar muisklikken toevoegt. De module biedt ook een set van vooraf ingevulde templates van veelvoorkomende verwerkingsactiviteiten vanuit de FORA, eventueel onderverdeeld in verschillende procescategorieën. We hebben bijna 300 juridisch getoetste standaardtemplates toegevoegd voor de meest voorkomende verwerkers in het funderend onderwijs.

Dienst Verwerkersovereenkomsten (DV) - Kennisnet

De Dienst Verwerkersovereenkomsten (DV) van Kennisnet faciliteert de digitale ondertekening van de verwerkingsovereenkomst tussen de verwerkingsverantwoordelijke (schoolbestuur) en de verwerker. Met alleen een getekende verwerkersovereenkomst voldoe je echter nog niet aan het verplichte register van verwerkingsactiviteiten. YourSafetynet RVV biedt de mogelijkheid om de ondertekende verwerkersovereenkomst te koppelen (uploaden) aan de juridisch getoetste templates over deze verwerker. Als de BIV-classificatie na deze koppeling aanleiding geeft om een DPIA uit te voeren, wordt de verwerking als zodanig in de tool gemarkeerd.

Meer info: www.yoursafetynet.com/rvv

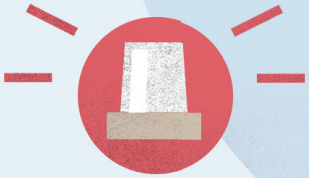
Met YourSafetynet RVV is het opzetten en bijhouden van een Register van Verwerkingen snel en eenvoudig geregeld.

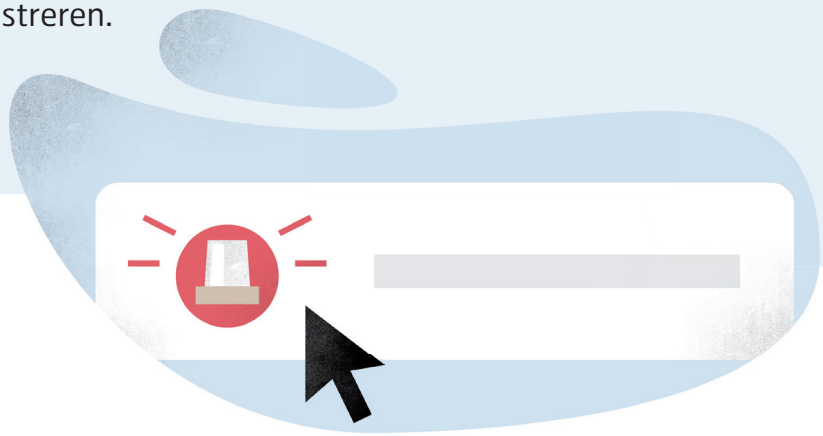
Meer info: yoursafetynet.com/sim

YourSafetynet SIM

Register van beveiligingsincidenten

Het melden van beveiligingsincidenten en datalekken kan voor veel onderwijsinstellingen een ingewikkeld proces zijn. Het is echter van cruciaal belang dat verantwoordelijken op tijd op de hoogte zijn van alle incidenten en meldingen om aan hun verplichtingen te voldoen en verbeteringen aan te brengen in hun beveiliging en beleid. Om deze reden biedt YourSafetynet IBP een oplossing in de vorm van YourSafetynet SIM (Security Incident Management). Hiermee kun je beveiligingsincidenten en datalekken eenvoudig melden en registreren.





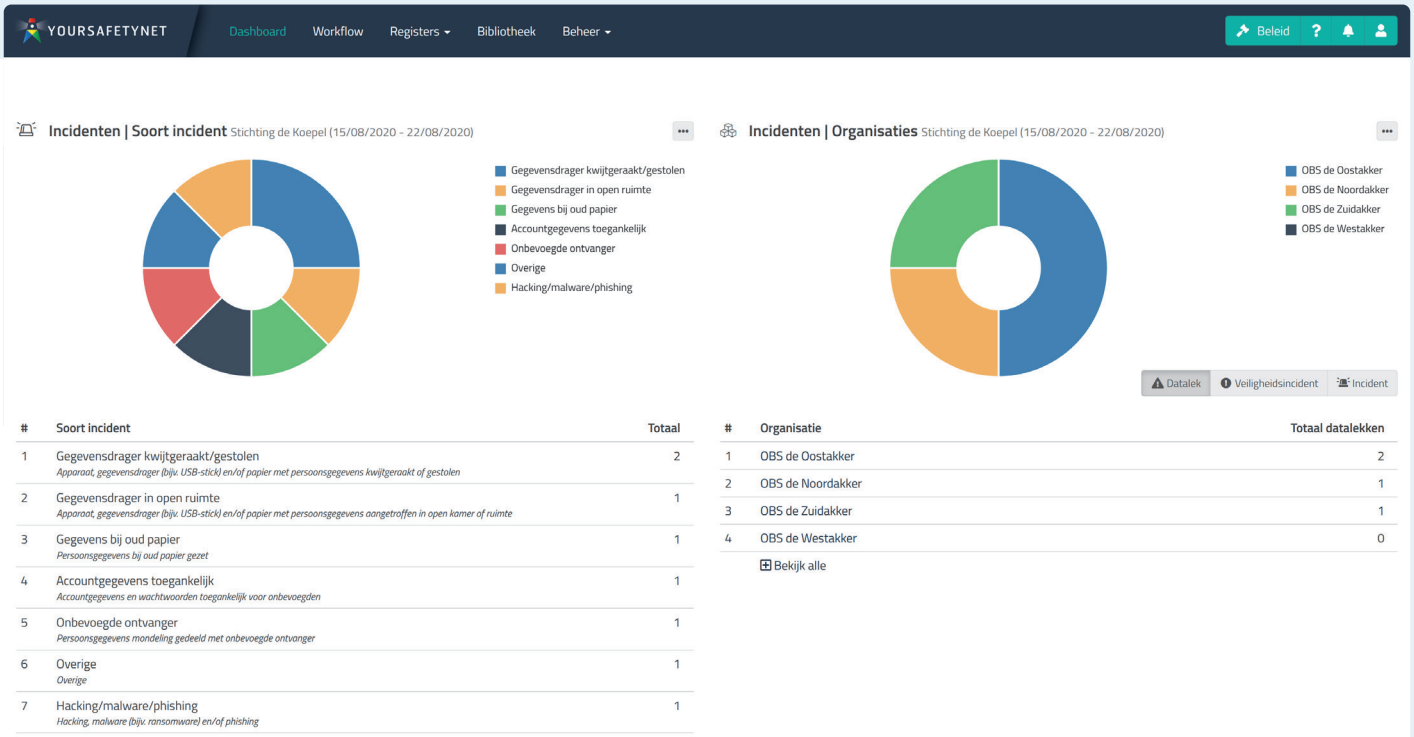
→ Met YourSafetynet SIM meld je eenvoudig een veiligheidsincident via de meldknop. Ook via je smartphone.

Incidenten melden

In de praktijk worden incidenten vaak gemeld door medewerkers. Met YourSafetynet SIM kunnen alle betrokkenen binnen de organisatie snel en met minimale inspanning beveiligingsincidenten en datalekken melden. De melding wordt vervolgens langs een specifieke route geleid die is afgestemd op de onderwijsinstelling. Tijdens deze route kunnen de verantwoordelijke partijen de melding verder verwerken en indien nodig toelichting geven en/of maatregelen vastleggen conform de eisen van de AVG (art. 33 lid 5).

Snelkoppeling

Beveiligingsincidenten kunnen worden gemeld via een meldknop die leidt naar een (publiek) formulier op het intranet van de onderwijsinstelling. Dit formulier kun je ook als handige snelkoppeling op een desktop of startscherm van mobiel of tablet plaatsen. Alle meldingen worden verwerkt en gecategoriseerd in het register van beveiligingsincidenten. Gedurende dit proces stuurt de incident manager specifieke notificaties naar de verantwoordelijke personen van de onderwijsinstelling. Het beschikbare dashboard biedt een volledige visuele rapportage van de beveiligingsincidenten die hebben plaatsgevonden.



#	Soort incident	Totaal
1	Gegevensdrager kwijtgeraakt/gestolen *Apparaat, gegevensdrager (bijv. USB-stick) en/of papier met persoonsgegevens kwijtgeraakt of gestolen*	2
2	Gegevensdrager in open ruimte *Apparaat, gegevensdrager (bijv. USB-stick) en/of papier met persoonsgegevens aangetroffen in open kamer of ruimte*	1
3	Gegevens bij oud papier *Persoonsgegevens bij oud papier gezet*	1
4	Accountgegevens toegankelijk *Accountgegevens en wachtwoorden toegankelijk voor onbevoegden*	1
5	Onbevoegde ontvanger *Persoonsgegevens mondeling gedeeld met onbevoegde ontvanger*	1
6	Overige *Overige*	1
7	Hacking/malware/phishing *Hacking, malware (bijv. ransomware) en/of phishing*	1

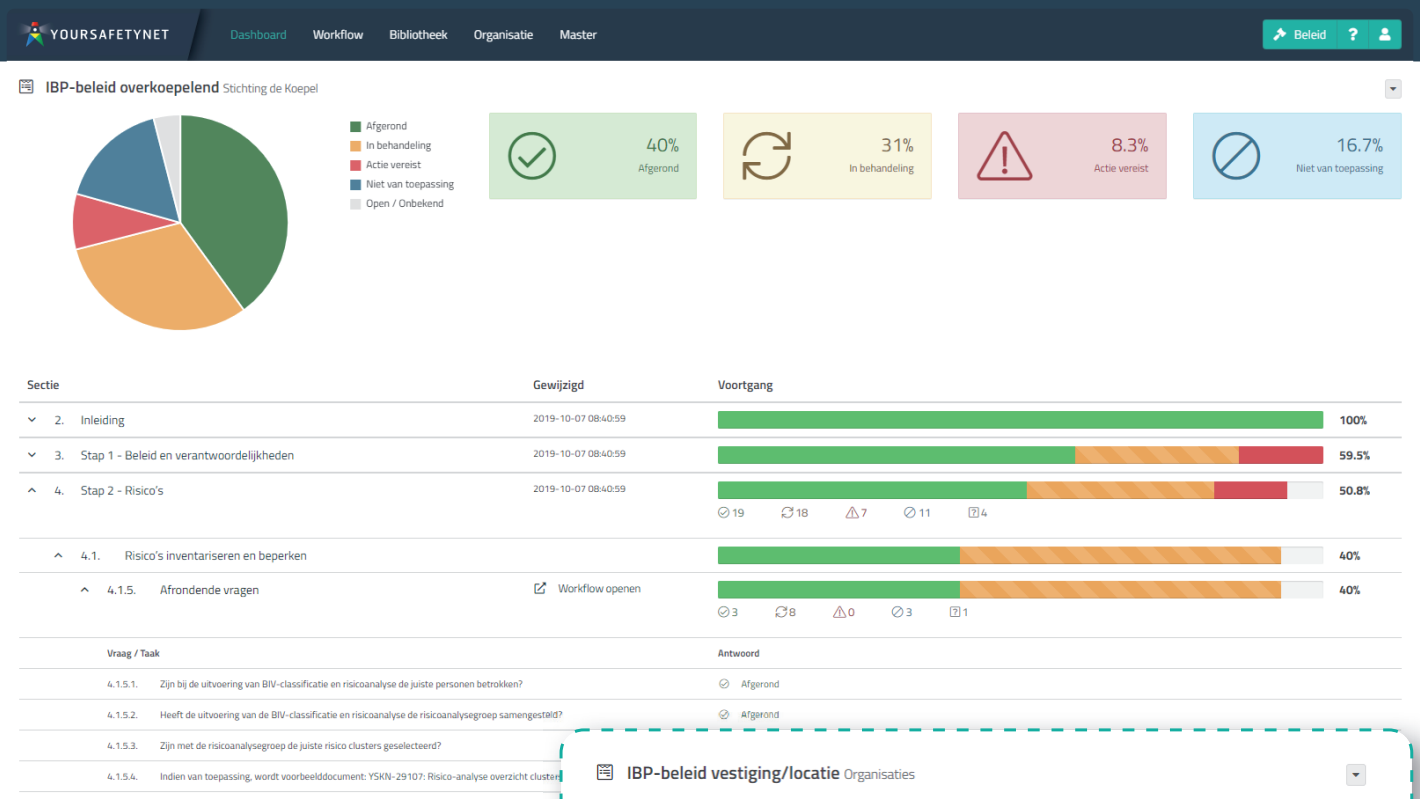
#	Organisatie	Totaal datalekken
1	OBS de Oostakker	2
2	OBS de Noordakker	1
3	OBS de Zuidakker	1
4	OBS de Westakker	0

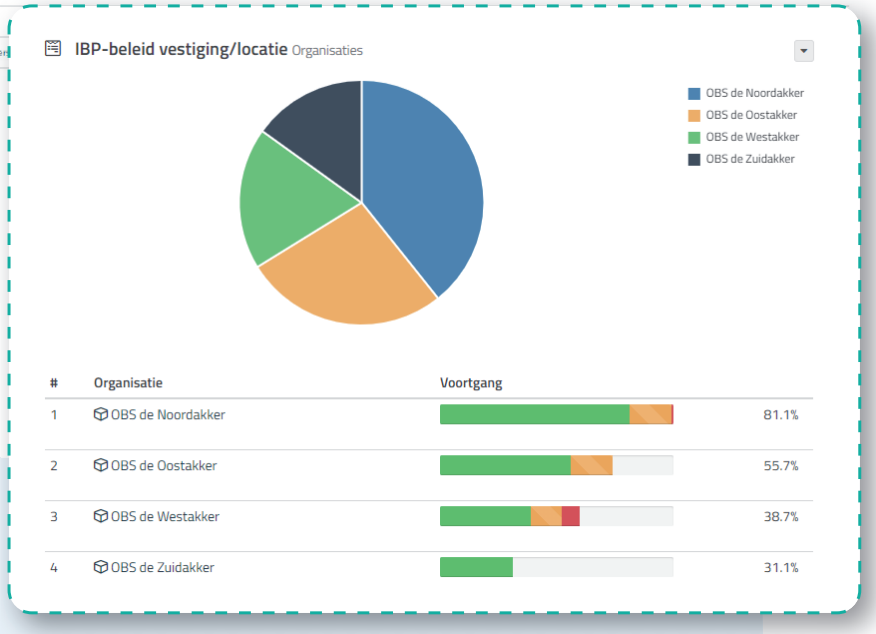
Bekijk alle

→ YourSafetynet SIM biedt snel inzicht in het type en de hoeveelheid veiligheidsincidenten per locatie.

Blijvend ‘in control’ dankzij de PDCA-cyclus

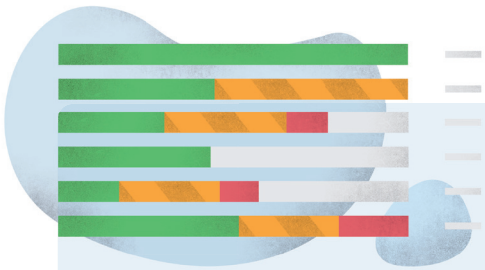
Het is vaak onduidelijk wat de precieze status van een IBP-traject is. Welke stappen zijn al gezet en welke nog niet? Is er bewijsvoering beschikbaar? Zijn de uitgevoerde activiteiten getoetst? Wat is de planning voor het komende jaar? Welke activiteiten keren regelmatig terug? Informatiebeveiliging en privacy is een continu proces en om dit proces effectief te beheren is de PDCA-cyclus (Plan-Do-Check-Act) geïntegreerd in de workflow. Dit maakt het mogelijk om stap voor stap taken, planning, prioriteiten, acties en daarmee processen, prestaties en instellingen continu te verbeteren.





→ De tooling biedt een overzicht van de uitvoering en implementatie van IBP-werkzaamheden.

→ Voor elke vestiging/locatie kun je de status en voortgang van toegewezen taken inzien.



Rapporteren

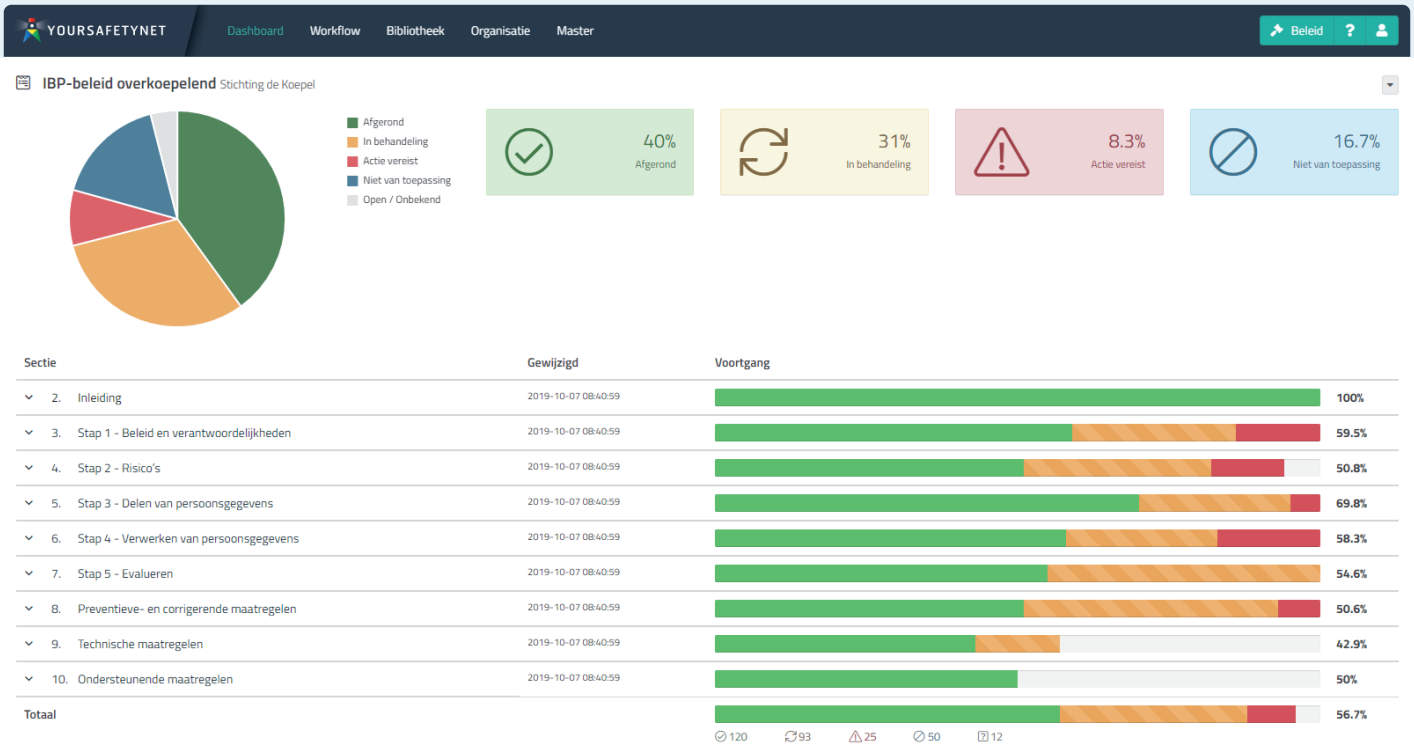
Met behulp van heldere rapportages hebben verantwoordelijken (zoals het CvB) en andere betrokkenen, waaronder accountants, een duidelijk en compleet zicht op de uitvoering en implementatie van IBP-werkzaamheden. Bovendien is een regelmatige evaluatie en actualisering van taken ook opgenomen in de tooling.

Presenteren

Onze tooling presenteert kwartiermakers, privacy officers, de functionarissen voor de gegevensbescherming en bestuurders fijnmazig inzicht in de voortgang en status van de te nemen IBP-maatregelen.

Operationele functies

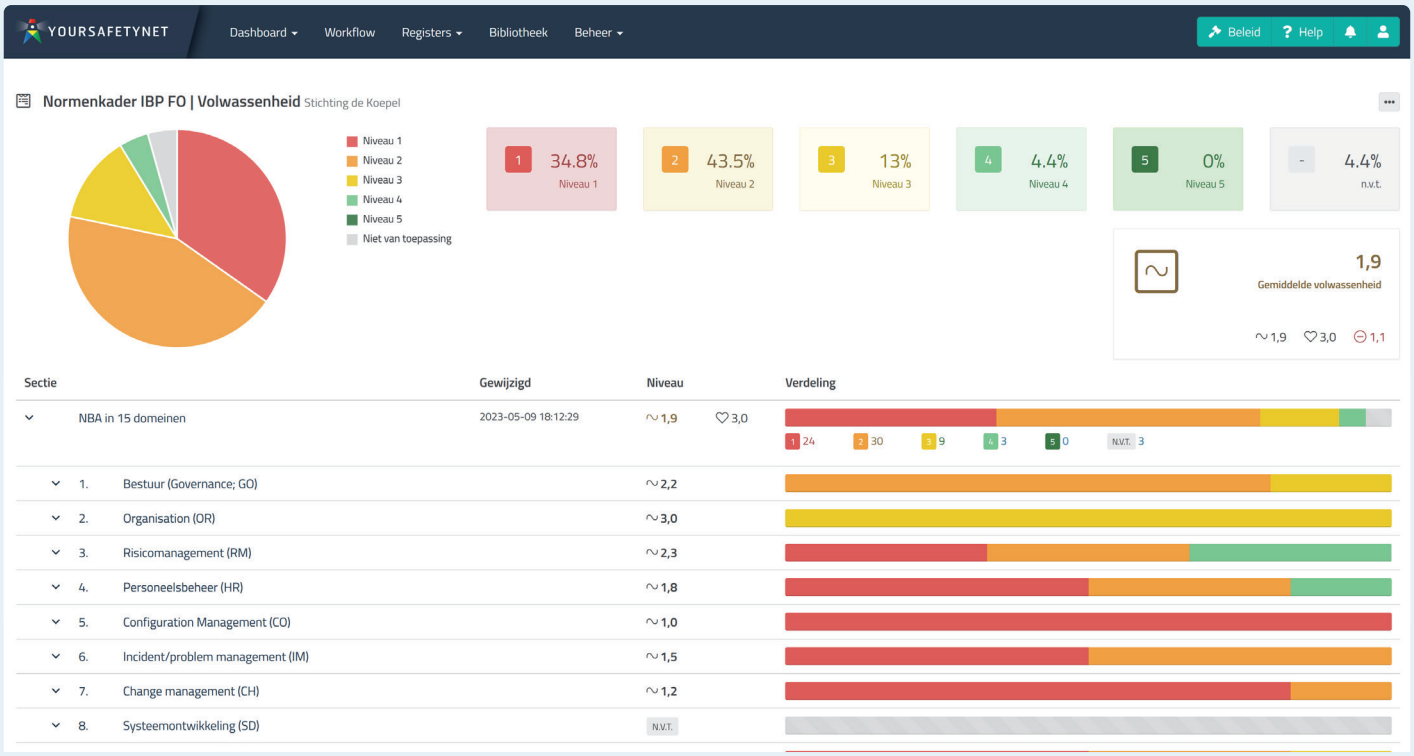
Hoe ver is het IBP-traject gevorderd en zijn er vertragingen? Wat zijn de grootste risico's die we als eerste moeten aanpakken? Met de overzichtelijke dashboards krijgen kwartiermakers, privacy officers, functionarissen gegevensbescherming en bestuurders snel inzicht in de status van de statements binnen de workflow. Zo wordt direct duidelijk welke taken en maatregelen zijn gestart, welke vertraging hebben opgelopen en welke juist zijn afgerond. Het volwassenheidsniveau van de deelgebieden uit het normenkader is ook direct inzichtelijk. Hierdoor behoudt men altijd grip op het traject en kan er tijdig worden bijgestuurd door de verantwoordelijken.



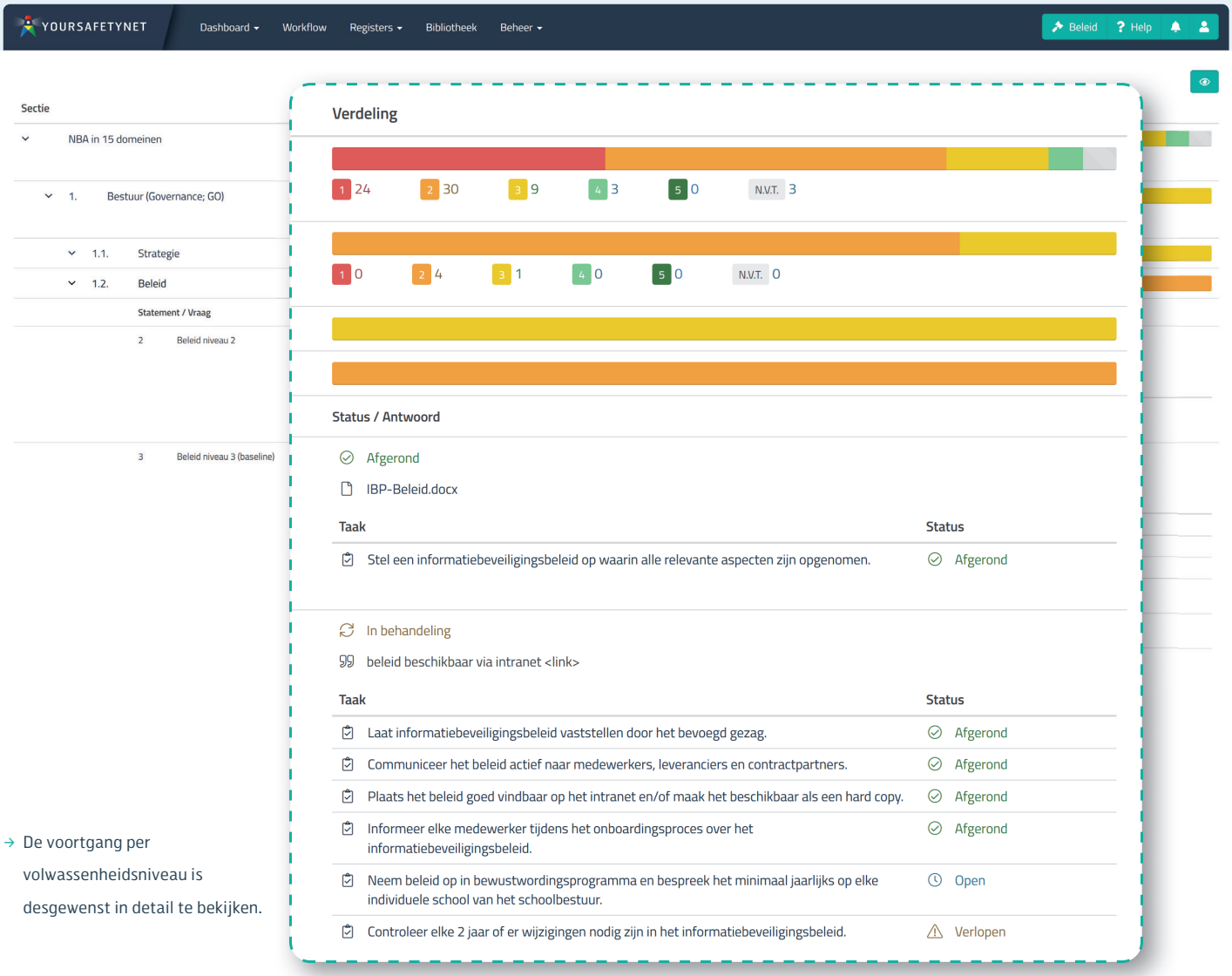
→ De oplossing geeft een gedetailleerd overzicht van de uitvoering en implementatie van IBP-werkzaamheden.

Overzichtelijke status-dashboards

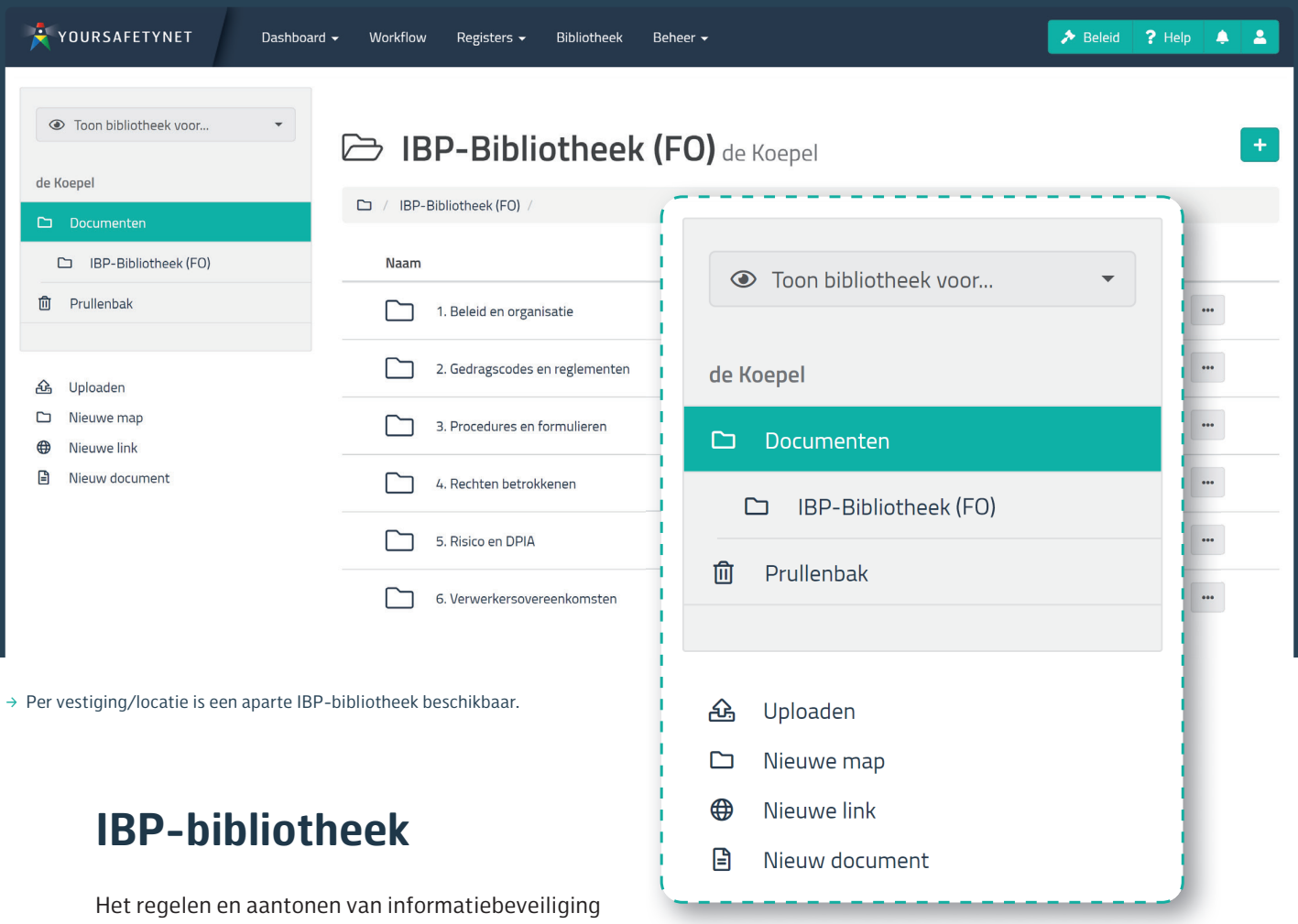
De statusdashboards geven ook inzicht voor onderwijsinstellingen met meerdere vestigingen of locaties. Voor iedere vestiging kunnen binnen de IBP-workflow taken en opdrachten worden uitgezet, waarvan de voortgangsstatus ook in het dashboard is te zien. Zo kan het bestuur en de FG op beleidsniveau precies zien wat de voortgang van de uit te voeren stappen is. Regelmatige evaluatie en actualisering zijn eveneens taken die in de tooling zijn opgenomen.



→ De oplossing biedt een compleet overzicht van de voortgang rondom het volwassenheidsniveau van IBP-werkzaamheden



→ De voortgang per volwassenheidsniveau is desgewenst in detail te bekijken.



→ Per vestiging/locatie is een aparte IBP-bibliotheek beschikbaar.

IBP-bibliotheek

Het regelen en aantonen van informatiebeveiliging en privacy vereist administratieve verantwoording. Alle verantwoordingsdocumentatie kan eenvoudig en veilig worden bewaard in de centrale cloud-bibliotheek van YourSafetynet. Dit vergroot het overzicht en maakt het veel gemakkelijker om aan te tonen dat alles goed geregeld is.

> **Per vestiging/locatie is een aparte IBP-bibliotheek beschikbaar.**

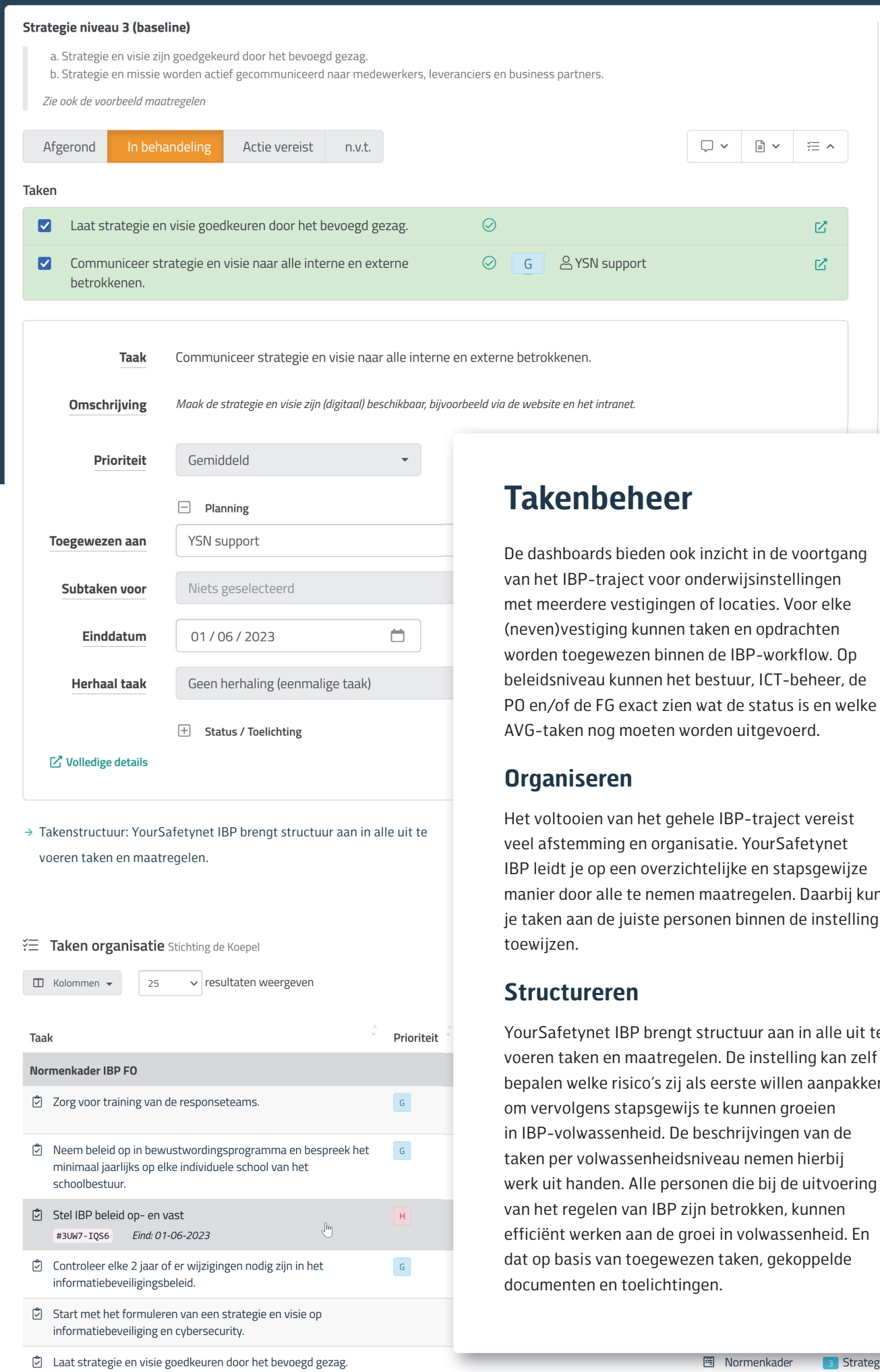
Flexibel toepasbaar en eenvoudig bestanden opslaan

De bibliotheek is standaard voorzien van een logische mappenstructuur, die bovendien volledig naar eigen inzicht kan worden aangepast. Verantwoordelijken kunnen de mappen naar wens hernoemen, verwijderen, aanmaken en kopiëren. De omgeving is geschikt voor het uploaden van PDF- en Office-documenten, archiefbestanden en afbeeldingen. Daarnaast heeft de organisatie nog altijd de mogelijkheid om binnen de bibliotheek te werken met een weblink naar de opslagplaats in de eigen omgeving, of een combinatie van beide. De oplossing biedt een veilige opslagvoorziening, gehost binnen de Europese Economische Ruimte (EER), waarin alle privacy-gerelateerde documenten kunnen worden bewaard.

IBP-documenten delen vanuit één centrale bibliotheek

De bibliotheek heeft ook een organisatorische functie. Vanuit deze bibliotheek kunnen verantwoordelijken documenten, sjablonen, weblinks of afspraken delen met verschillende afdelingen, vestigingen of locaties. Deze functie werkt ook voor documenten die buiten de tooling zijn aangemaakt. Ook kunnen op deze manier bestaande beleidsdocumenten en procedures een plaats krijgen in de centrale bibliotheek.

> **YourSafetynet brengt structuur aan in de uit te voeren taken en maatregelen**



Takenbeheer

De dashboards bieden ook inzicht in de voortgang van het IBP-traject voor onderwijsinstellingen met meerdere vestigingen of locaties. Voor elke (neven)vestiging kunnen taken en opdrachten worden toegewezen binnen de IBP-workflow. Op beleidsniveau kunnen het bestuur, ICT-beheer, de PO en/of de FG exact zien wat de status is en welke AVG-taken nog moeten worden uitgevoerd.

Organiseren

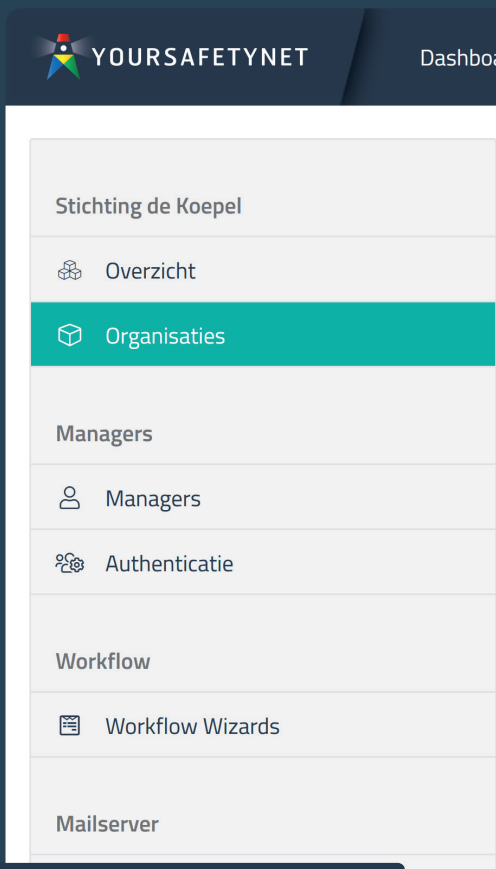
Het voltooien van het gehele IBP-traject vereist veel afstemming en organisatie. YourSafetynet IBP leidt je op een overzichtelijke en stapsgewijze manier door alle te nemen maatregelen. Daarbij kun je taken aan de juiste personen binnen de instelling toewijzen.

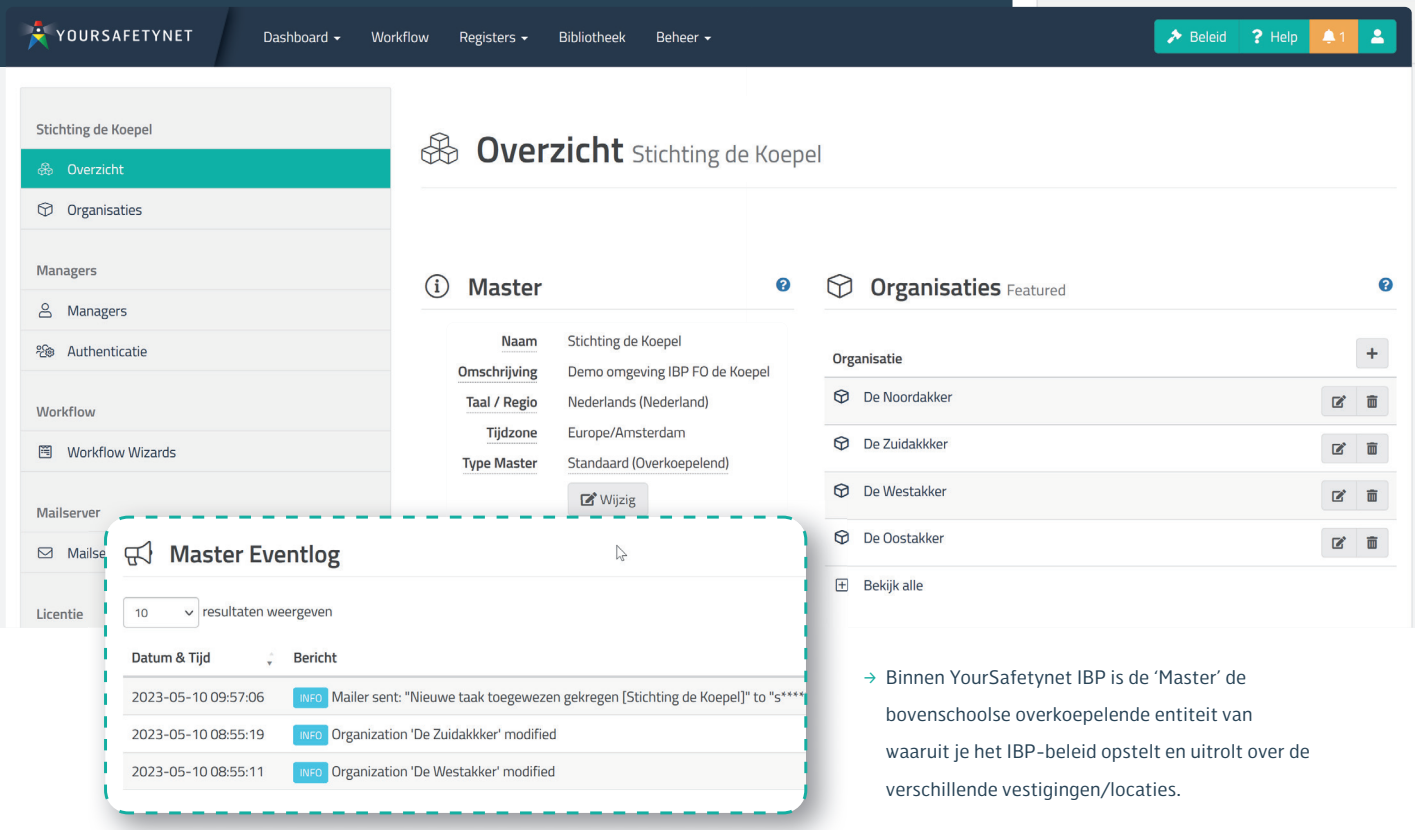
Structureren

YourSafetynet IBP brengt structuur aan in alle uit te voeren taken en maatregelen. De instelling kan zelf bepalen welke risico's zij als eerste willen aanpakken om vervolgens stapsgewijs te kunnen groeien in IBP-volwassenheid. De beschrijvingen van de taken per volwassenheidsniveau nemen hierbij werk uit handen. Alle personen die bij de uitvoering van het regelen van IBP zijn betrokken, kunnen efficiënt werken aan de groei in volwassenheid. En dat op basis van toegewezen taken, gekoppelde documenten en toelichtingen.

Beheer

YourSafetynet IBP is op het moment van ingebruikname volledig afgestemd op de geldende organisatiestructuur van de onderwijsinstelling. Hierdoor kunnen betrokken medewerkers na de juiste instructies snel en efficiënt aan de slag. Niet alleen de organisatiestructuur wordt vastgelegd, maar ook de rollen, taken en verantwoordelijkheden van de betrokken personen.

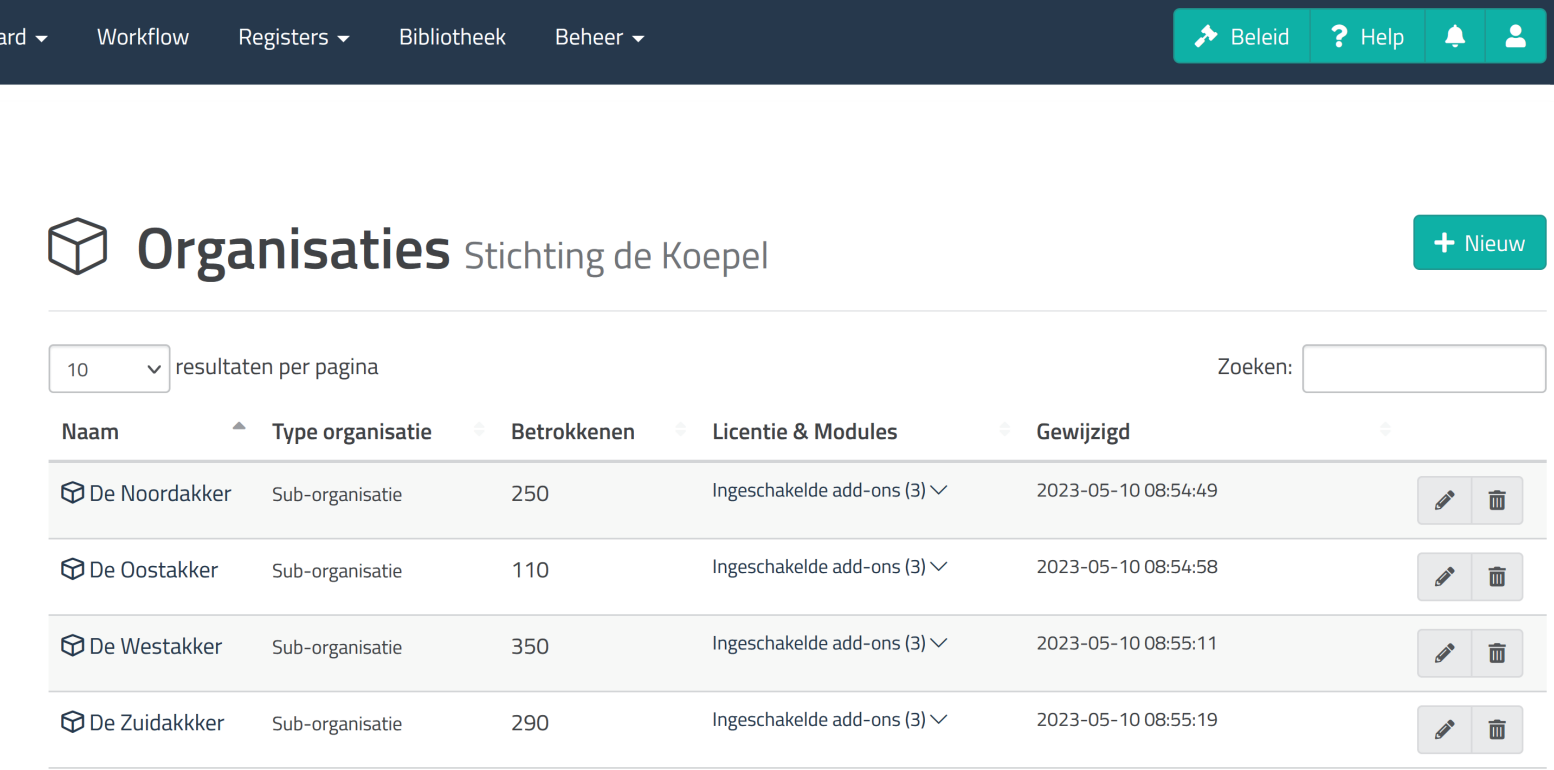


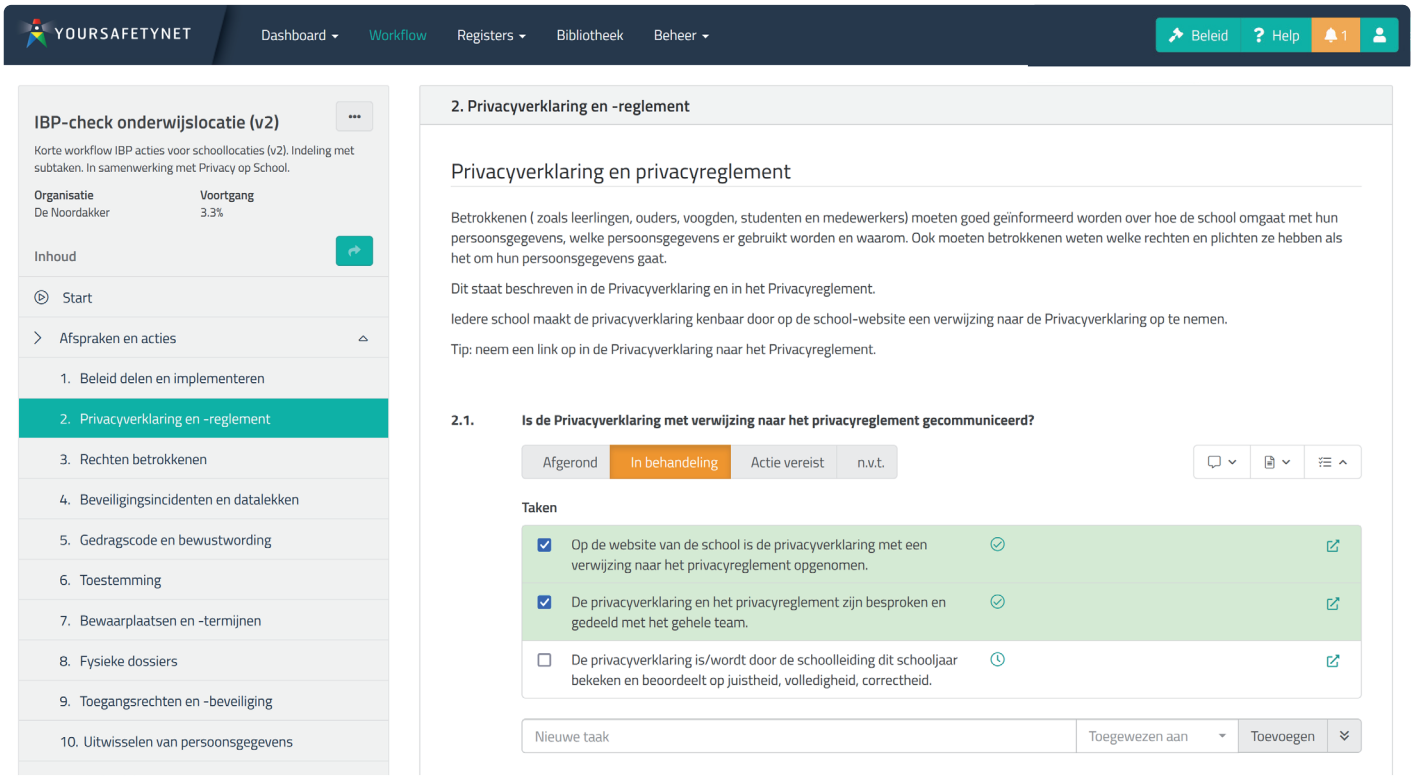


→ Binnen YourSafetynet IBP is de 'Master' de bovenschoolse overkoepelende entiteit van waaruit je het IBP-beleid opstelt en uitrolt over de verschillende vestigingen/locaties.

Master (bovenschools)

Binnen YourSafetynet IBP is de 'Master' de bovenschoolse overkoepelende entiteit. Om deze strategische aanpak te ontwikkelen op bestuursniveau wordt meestal samengewerkt met de BIC/ICT-manager, de privacy officer en HR, waarbij de FG om advies wordt gevraagd. Dit vereist een integrale en overkoepelende aanpak waarbij alle benodigde aandacht wordt besteed aan het identificeren van risico's, het nemen van beschermende maatregelen, het detecteren van incidenten, het reageren op incidenten wanneer ze zich voordoen en het herstellen van eventuele schade.

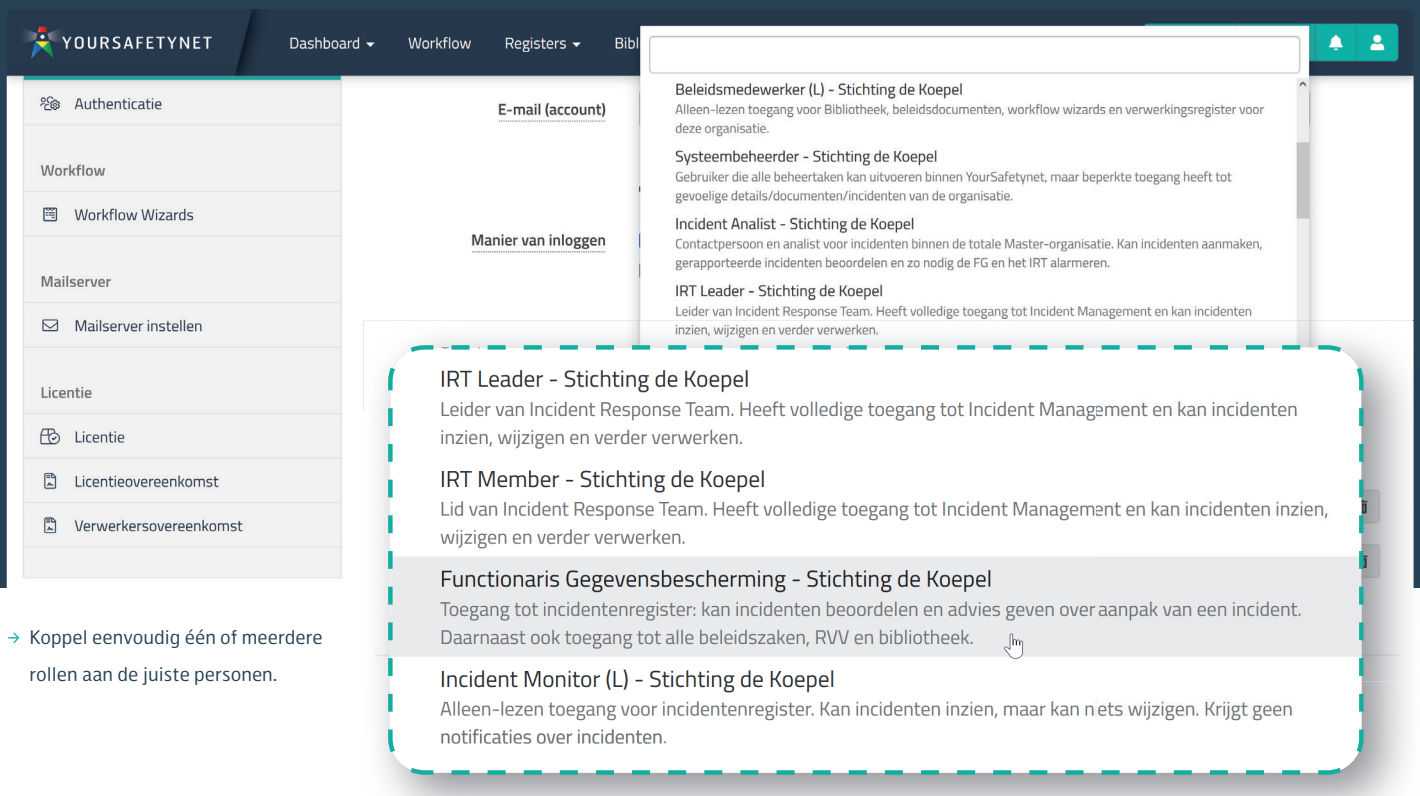




→ Voor de individuele scholen is er een specifieke wizard beschikbaar op school-/vestigingsniveau.

Organisatie (vestigingen/locaties)

Voor de individuele scholen is er een specifieke wizard beschikbaar op school-/vestigingsniveau. Hiermee kun je documenten en taken koppelen, eventueel met een doorlooptijd. Het uitgangspunt daarbij is om de afzonderlijke scholen zo min mogelijk te belasten met onnodige of dubbele werkzaamheden en ingewikkelde materie. Elke locatie kan stap voor stap aangeven in hoeverre de bovenschoolse afspraken/procedures zijn geïmplementeerd.

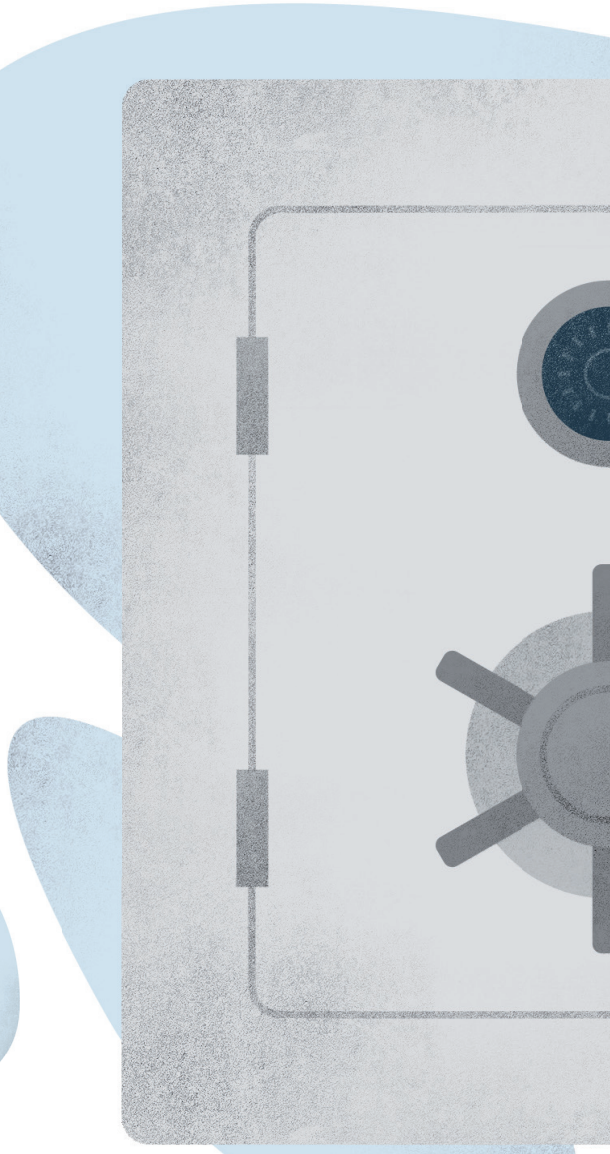


→ Koppel eenvoudig één of meerdere rollen aan de juiste personen.

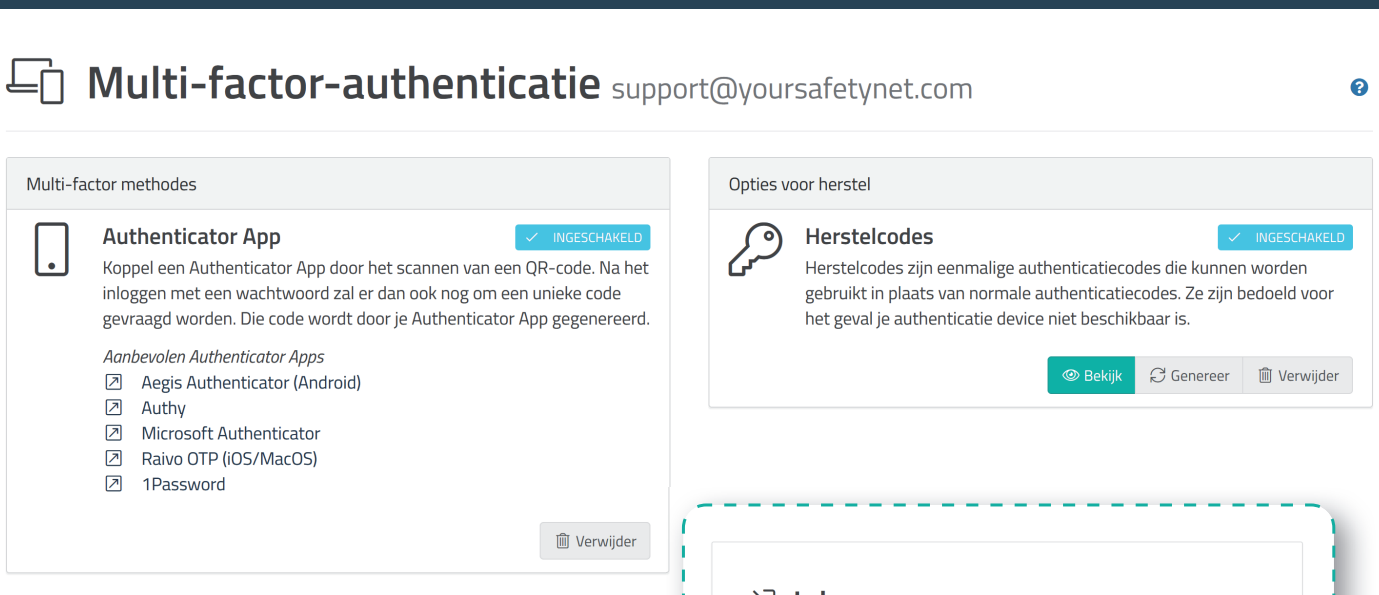
Rollen en rechten

Binnen de onderwijsinstelling hebben personen specifieke rollen, taken en verantwoordelijkheden als het gaat om informatiebeveiliging en privacy. Afhankelijk van de manier waarop een onderwijsinstelling is georganiseerd, kan de uitvoering van IBP bij meerdere medewerkers in de organisatie worden belegd.

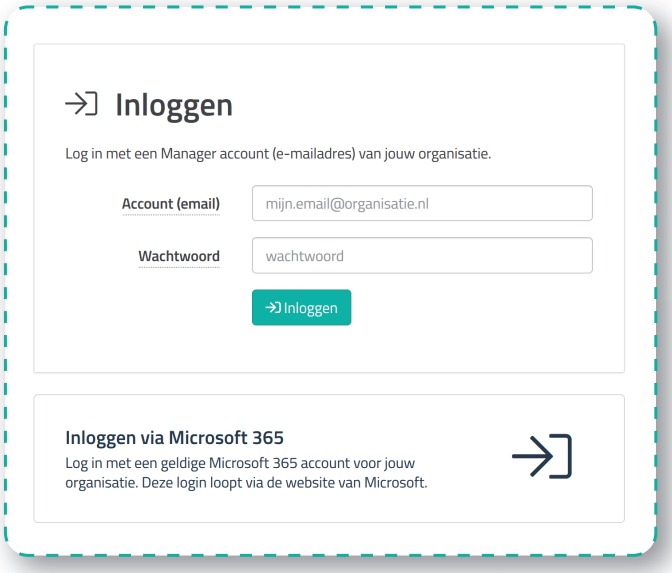
Binnen YourSafetynet hebben gebruikers daarom verschillende (functie)rollen. Een gebruiker kan één of meer rollen toegewezen krijgen. Afhankelijk van de rol heeft de gebruiker wel of geen rechten op het uitvoeren van een bepaalde taak, of inzien van bepaalde gegevens. Stel iemand heeft een breed takenpakket, dan kan de persoon meerdere rollen tegelijkertijd nodig hebben. Doet iemand het werk bij meerdere vestigingen/locaties, dan kan die persoon bij al die sub-organisaties zijn eigen rollen hebben.



Koppel eenvoudig één of meerdere rollen aan de juiste personen.

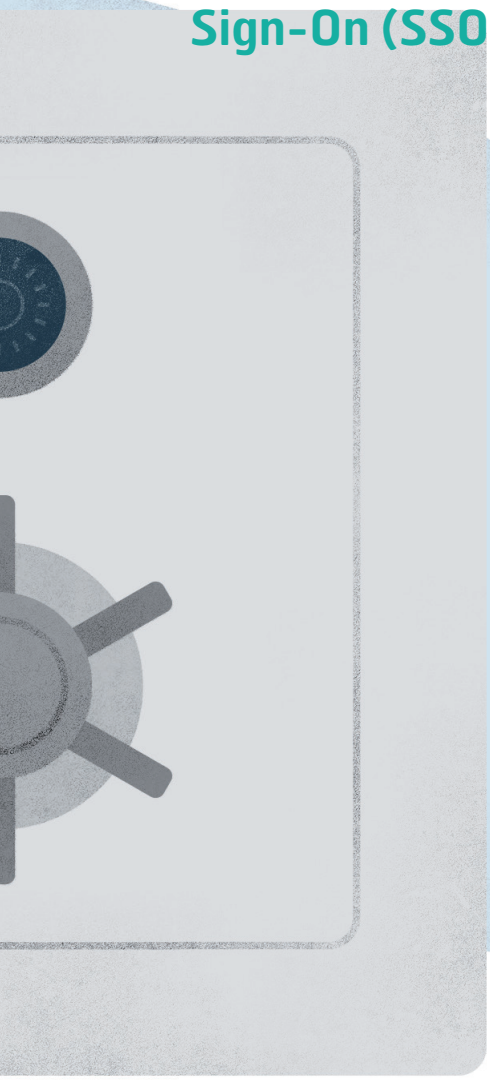


→ MFA verkleint de kans sterk dat onbevoegden toegang krijgen tot de IBP-omgeving.



→ Gebruikers loggen eenvoudig in dankzij Microsoft 365 Single Sign-On

Gebruikers loggen eenvoudig in dankzij Microsoft 365 Single Sign-On (SSO)

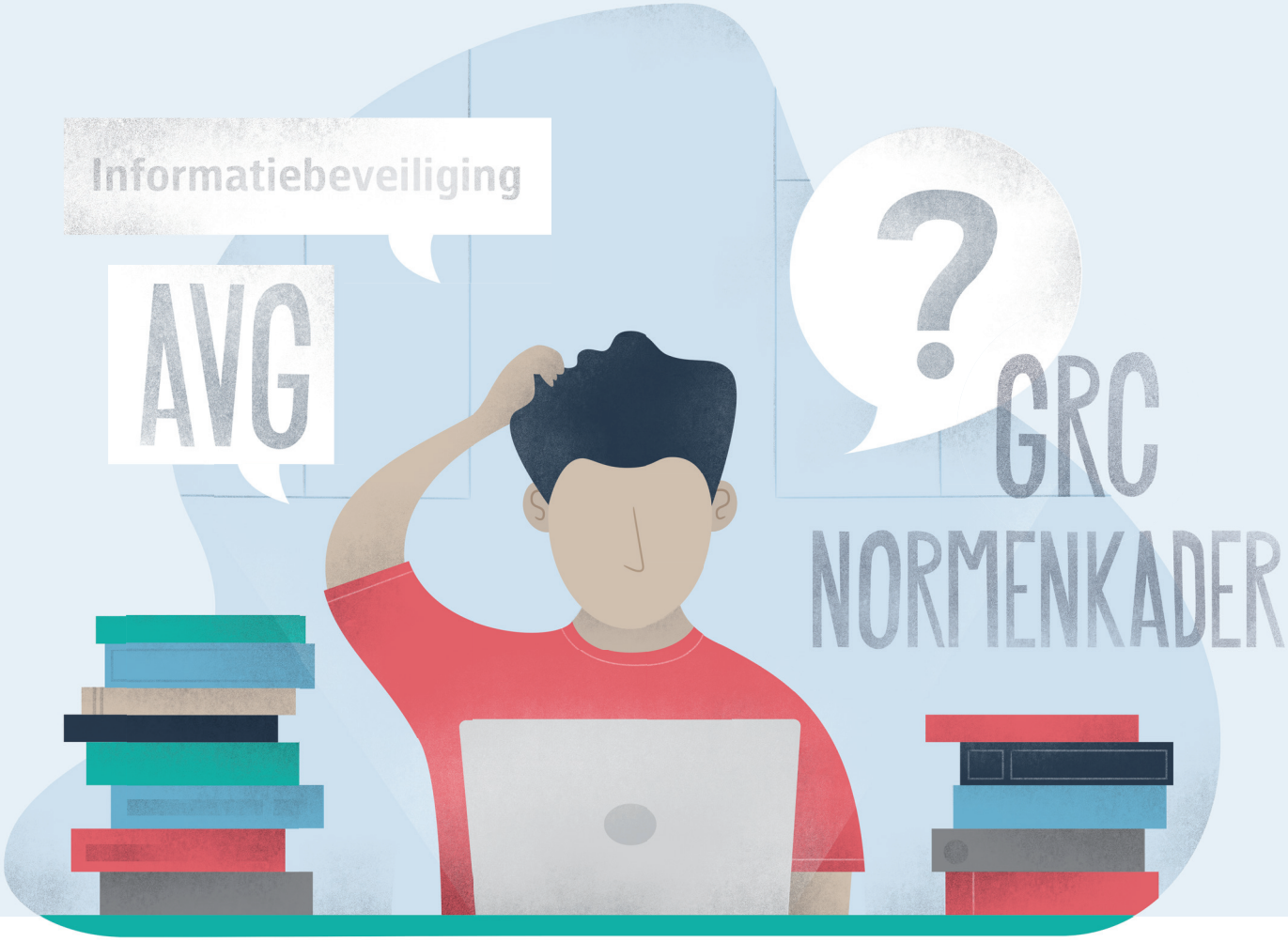


Multi-factorauthenticatie (MFA)

Een ketting is net zo sterk als de zwakste schakel. Daarom is YourSafetynet IBP uitgevoerd met multi-factorauthenticatie (MFA). Naast het invoeren van hun account en wachtwoord, moeten gebruikers ook een extra verificatiecode invoeren die bijvoorbeeld gegenereerd wordt via een authenticator app op hun smartphone.

Microsoft 365 Single Sign-On

Veel organisaties maken gebruik van Microsoft 365. Bij YourSafetynet IBP hoef je niet “weer” een nieuw account en wachtwoord te maken. In plaats daarvan kun je inloggen met je Microsoft 365-account van de onderwijsinstelling (Single Sign-On).



Benieuwd naar de voordelen van YourSafetynet voor jouw onderwijsinstelling?

Ga naar yoursafetynet.com/onderwijs voor meer informatie.

Vragen of een ‘live’ demonstratie van de mogelijkheden?

Neem direct contact op via 085 06 04 116 of contact@yoursafetynet.com.

YOURSAFETYNET

Informatiebeveiliging & Privacy.
Snel. Eenvoudig. Zonder gedoe.